Published since January 1947 and Published before May 1999
Terms used **oblivious signature proof prover verifier**

Found **59** of **86,160**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 59 Result page: **1** 2 3 next

Relevance scale

considered

1 Linear zero-knowledge—a note on efficient zero-knowledge proofs and arguments
Ronald Cramer, Ivan Damgård
May 1997 **Proceedings of the twenty-ninth annual ACM symposium on Theory of computing**
Full text available: pdf(1.47 MB) Additional Information: full citation, references, index terms

considered

2 On randomization in sequential and distributed algorithms
Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

considered

3 Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems
Oded Goldreich, Silvio Micali, Avi Wigderson
July 1991 **Journal of the ACM (JACM)**, Volume 38 Issue 3
Full text available: pdf(3.04 MB) Additional Information: full citation, references, citings, index terms

Keywords: NP, cryptographic protocols, fault tolerant distributed computing, graph isomorphism, interactive proofs, methodological design of protocols, one-way functions, proof systems, zero-knowledge

4 Resettable zero-knowledge (extended abstract)
Ran Canetti, Oded Goldreich, Shafi Goldwasser, Silvio Micali
May 1999 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**

Full text available: pdf(1.21 MB) Additional Information: full citation, references, citings, index terms

Keywords: concurrent zero-knowledge, identification schemes, public-key cryptography, smart cards, witness-indistinguisable proofs, zero-knowledge

5 Verifiable partial key escrow
Mihir Bellare, Shafi Goldwasser
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(1.98 MB) Additional Information: full citation, references, index terms

Considered

6 Server-assisted cryptography
Donald Beaver
January 1998 **Proceedings of the 1998 workshop on New security paradigms**
Full text available: pdf(1.13 MB) Additional Information: full citation, references, citings, index terms

7 Robust efficient distributed RSA-key generation
Yair Frankel, Philip D. MacKenzie, Moti Yung
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**
Full text available: pdf(1.47 MB) Additional Information: full citation, references, citings, index terms

considered

8 On the complexity of verifiable secret sharing and multiparty computation
Ronald Cramer, Ivan Damgård, Stefan Dziembowski
May 1999 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**
Full text available: pdf(1.13 MB) Additional Information: full citation, references, citings, index terms

9 Optimal efficiency of optimistic contract signing
Birgit Pfitzmann, Matthias Schunter, Michael Waidner
June 1998 **Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing**
Full text available: pdf(1.40 MB) Additional Information: full citation, references, citings, index terms

10 Commodity-based cryptography (extended abstract)
Donald Beaver
May 1997 **Proceedings of the twenty-ninth annual ACM symposium on Theory of computing**
Full text available: pdf(1.33 MB) Additional Information: full citation, references, citings, index terms

11 25 years of quantum cryptography
Gilles Brassard, Claude Crépeau
September 1996 **ACM SIGACT News**, Volume 27 Issue 3
Full text available: pdf(918.87 KB) Additional Information: full citation, abstract, citings, index terms

The fates of *SIGACT News* and Quantum Cryptography are inseparably entangled. The exact date of Stephen Wiesner's invention of "conjugate coding" is unknown but it cannot be far from April 1969, when the premier issue of *SIGACT News*---or rather *SICACT News* as it was known at the time---came out. Much later, it was in *SIGACT News* that Wiesner's paper finally appeared [74] in the wake of the first author's early collaboration with Charles H. Bennett [7]. It was also in < ...

[12] On approximating arbitrary metrices by tree metrics
Yair Bartal
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**
Full text available: pdf(4.11 MB) Additional Information: full citation, references, citings, index terms

considered

[13] Secure computation with honest-looking parties (extended abstract): what if nobody is truly honest?
Ran Canetti, Rafail Ostrovsky
May 1999 **Proceedings of the thirty-first annual ACM symposium on Theory of computing**
Full text available: pdf(938.61 KB) Additional Information: full citation, references, index terms

[14] A simple, comprehensive type system for Java bytecode subroutines
Robert O'Callahan
January 1999 **Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**
Full text available: pdf(909.09 KB) Additional Information: full citation, references, citings, index terms

Keywords: Java, bytecode, continuations, polymorphic recursion, subroutines, types

[15] Oblivious data structures: applications to cryptography
Daniele Micciancio
May 1997 **Proceedings of the twenty-ninth annual ACM symposium on Theory of computing**
Full text available: pdf(1.49 MB) Additional Information: full citation, references, citings, index terms

[16] A theory of using history for equational systems with applications
Rakesh M. Verma
September 1995 **Journal of the ACM (JACM)**, Volume 42 Issue 5
Full text available: pdf(2.70 MB) Additional Information: full citation, abstract, references, index terms, review

Implementation of programming language interpreters, proving theorem of the form A=B, implementation of abstract data types, and program optimization are all problems that can be reduced to the problem of finding a normal form for an expression with respect to a finite set of equations. In 1980, Chew proposed an elegant congruence closure based simplifier (CCNS) for computing with regular systems, which stores the history of it computations in a compact data structure. In 1990, Verma and Ra ...

Keywords: congruence-closure algorithm, equational logic, proof theory, rewrite system transformation, term rewrite systems

[17] Incremental cryptography and application to virus protection
Mihir Bellare, Oded Goldreich, Shafi Goldwasser
May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of computing**
Full text available: pdf(1.65 MB) Additional Information: full citation, references, citings, index terms

considered

[18] A randomized protocol for signing contracts
Shimon Even, Oded Goldreich, Abraham Lempel
June 1985 **Communications of the ACM**, Volume 28 Issue 6
Full text available: pdf(1.23 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Randomized protocols for signing contracts, certified mail, and flipping a coin are presented. The protocols use a 1-out-of-2 oblivious transfer subprotocol which is axiomatically defined.The 1-out-of-2 oblivious transfer allows one party to transfer exactly one secret, out of two recognizable secrets, to his counterpart. The first (second) secret is received with probability one half, while the sender is ignorant of which secret has been received.An implementation of ...

considered

19 How to simultaneously exchange secrets by general assumptions 

Tatsuaki Okamoto, Kazuo Ohta

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Full text available: pdf(923.48 KB) Additional Information: full citation, abstract, references, citings, index terms

The simultaneous secret exchange protocol is the key tool for contract signing protocols and certified mail protocols. This paper proposes efficient simultaneous secret exchange protocols (or gradual secret releasing protocols) that are based on general assumptions such as the existence of one-way permutations and one-way functions, while the existing efficient simultaneous secret exchange protocols are based on more constrained assumptions such as specific number theoretic problems and the ...

20 Watermarking techniques for intellectual property protection 

A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, G. Wolfe

May 1998 **Proceedings of the 35th annual conference on Design automation conference**

Full text available: pdf(243.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital system designs are the product of valuable effort and know-how. Their embodiments, from software and HDL program down to device-level netlist and mask data, represent carefully guarded intellectual property (IP). Hence, design methodologies based on IP reuse require new mechanisms to protect the rights of IP producers and owners. This paper establishes principles of watermarking-based IP protection, where a watermark is a mechanism for identificatio ...

Results 1 - 20 of 59 Result page: **1** 2 3 next

Published since January 1947 and Published before May 1999
Term used **disavowal**

Found **26** of **86,160**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 26

Result page: **1** 2 next

Relevance scale

considered (1) Breaking and repairing a convertible undeniable signature scheme
Markus Michels, Holger Petersen, Patrick Horster
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(484.21 KB) Additional Information: full citation, references, index terms

2 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

considered (3) Sorting out signature schemes
Birgit Pfitzmann
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, citings, index terms

Digital signature schemes are a fundamental tool for secure distributed systems. It is important to have a formal notion of what a secure digital signature scheme is, so that there is a clear interface between designers and users of such schemes. A definition that seemed final was given by Goldwasser, Micali, and Rivest in 1988, and although most signature schemes used in practice cannot be proved secure with respect to it, they are all built so that they hopefully fulfil it, e.g., by the i ...

4 Asymmetric fingerprinting for larger collusions
Birgit Pfitzmann, Michael Waidner
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

considered (5) Proxy signatures for delegating signing operation
Masahiro Mambo, Keisuke Usuda, Eiji Okamoto
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

6

Security without identification: transaction systems to make big brother obsolete
David Chaum
October 1985 **Communications of the ACM**, Volume 28 Issue 10

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms, review

The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

7 Hart's critics on defeasible concepts and ascriptivism
Ronald P. Loui
May 1995 **Proceedings of the fifth international conference on Artificial intelligence and law**

Full text available: pdf(1.27 MB) Additional Information: full citation, references, citings, index terms

8 Stalking the paratext: speculations on hypertext links as a second order text
Francisco J. Ricardo
May 1998 **Proceedings of the ninth ACM conference on Hypertext and hypermedia : links, objects, time and space---structure in hypermedia systems: links, objects, time and space---structure in hypermedia systems**

Full text available: pdf(1.38 MB) Additional Information: full citation, references, citings, index terms

9 Computer science education and social relevance
Ben Shneiderman
March 1971 **ACM SIGCSE Bulletin**, Volume 3 Issue 1

Full text available: pdf(481.71 KB) Additional Information: full citation, abstract

The rise of computer science as a theoretical discipline should not be allowed to proceed without promoting the study of the social implications and applications of the field. This paper describes an undergraduate course whose primary goal is to foster an understanding of how computers can be used for socially relevant purposes. The students were required to propose and execute a project which could benefit people directly. The projects are described and suggestions for further work are given.Th ...

10 Segment transfer protocols for a homogeneous computer network
Eric Manning, R. W. Peebles
January 1975 **ACM SIGOPS Operating Systems Review , Proceedings of the 1975 ACM SIGCOMM/SIGOPS workshop on Interprocess communications**, Volume 9 Issue 3

Full text available: pdf(448.05 KB) Additional Information: full citation, abstract, references, index terms

This research is focussed on solving certain problems of distributed processing on a distributed data base, with emphasis on transaction processing. Many data bases exhibit geographic locality of reference; most of the transactions homing on a given component of the data base originate from a particular geographic region. At the same time there is a need to operate the collection of components as a single data base, to provide For occasional transactions which cross r ...

11 Cryptographic protocols
Richard A. DeMillo, Nancy A. Lynch, Michael J. Merritt
May 1982 **Proceedings of the fourteenth annual ACM symposium on Theory of computing**

Full text available: pdf(1.34 MB) Additional Information: full citation, abstract, references, citings

A cryptographic transformation is a mapping f from a set of cleartext messages, M, to a set of ciphertext messages. Since for m e M, f(m) should hide the contents of m from an enemy, f-1 should, in a certain technical sense, be difficult to infer from f(m) and public knowledge about f. A cryptosystem is a model of computation and communication which permits the manipulation of messages by cryptographic transformat ...

12 GRAP—a language for typesetting graphs
Jon L. Bentley, Brian W. Kernighan
August 1986

Communications of the ACM, Volume 29 Issue 8

Full text available: pdf(952.60 KB) Additional Information: full citation, abstract, references, citings, index terms

The authors describe a system that makes it easy and convenient to describe graphs and to include them as an integral part of the document formatting process.

13 Technical correspondence: on secure personal computing
Stephen T. Kent, Doug Bates
January 1980 **Communications of the ACM**, Volume 23 Issue 1

Full text available: pdf(726.72 KB) Additional Information: full citation, references

14 Symmetric and Asymmetric Encryption
Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

15 Cryptology in Transition
Abraham Lempel
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Full text available: pdf(1.63 MB) Additional Information: full citation, references, citings, index terms

16 Timestamps in key distribution protocols
Dorothy E. Denning, Giovanni Maria Sacco
August 1981 **Communications of the ACM**, Volume 24 Issue 8

Full text available: pdf(397.16 KB) Additional Information: full citation, abstract, references, citings, index terms

The distribution of keys in a computer network using single key or public key encryption is discussed. We consider the possibility that communication keys may be compromised, and show that key distribution protocols with timestamps prevent replays of compromised keys. The timestamps have the additional benefit of replacing a two-step handshake.

Keywords: communications, encryption, encryption keys, key distribution, security, timestamps

17 A computer system for transformational grammar
Joyce Friedman
June 1969 **Communications of the ACM**, Volume 12 Issue 6

Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, references, citings, index terms

A comprehensive system for transformational grammar has been designed and implemented on the IBM 360/67 computer. The system deals with the transformational model of syntax, along the lines of Chomsky's Aspects of the Theory of Syntax. The major innovations include a full, formal description of the syntax of a transformational grammar, a directed random phrase structure generator, a lexical insertion algorithm, an extended definition of analysis, and a simple problem-orient ...

Keywords: computational linguistics, language analysis, language processing, lexical insertion, natural language syntax, sentence generation, syntax, transformational grammar

18 Signature simulation and certain cryptographic codes
Carl Hammer
January 1971 **Communications of the ACM**, Volume 14 Issue 1

Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references

Three cyphers allegedly authored by Thomas Jefferson Beale in 1822 have been the subject of intensive study for over 100 years. Generations of cryptanalysts have expended untold man-

years, thus far without success, attempting to decode them; vast armies of fortune hunters and treasure seekers have devoted Herculean labors to digging up the rolling hills of Virginia trying to locate the promised bonanza. The history of pertinent activities would fill volumes, yet serious students of cryptogr ...

Keywords: Declaration of Independence, Magna Carta, Thomas Jefferson Beale, codes, cryptanalysis, cyphers, decoding, encoding, pseudotext, signature, simulation

[19] Semantic Road Maps for Literature Searchers
Lauren B. Doyle
October 1961 **Journal of the ACM (JACM)**, Volume 8 Issue 4
Full text available: pdf(1.46 MB) Additional Information: full citation, references, citings, index terms

[20] ACM Forum
Robert L. Ashenhurst
May 1989 **Communications of the ACM**, Volume 32 Issue 5
Full text available: pdf(892.64 KB) Additional Information: full citation, references, index terms

Results 1 - 20 of 26 Result page: **1** 2 next